Обеспечение безопасности в сфере дистанционного банковского обслуживания в системе «Банк-Клиент» .

О хищениях и причинах их возникновения

В настоящее время в российских банках начался лавинообразный рост хищений денежных средств со счетов клиентов с использованием систем дистанционного банковского обслуживания (далее ДБО). Используя уязвимости в операционных системах, Web-браузерах и почтовых программах, злоумышленники заражают компьютеры клиентов вредоносными программами (троянами) и дистанционно используют секретные ключи ЭЦП клиентов и пароли, вводимые с клавиатуры.

Далее злоумышленники по системе дистанционного банковского обслуживания «Банк-Клиент» от имени клиента подключаются к банку, отслеживают поступления средств и в нужный момент направляют в банк платежные поручения с корректными ЭЦП клиента.

Кроме того, мошенническое платежное поручение создается, подписывается ЭЦП клиента (в том числе с использованием подключенного USB-токена или Смарт-карты) и отправляется в банк непосредственно на инфицированном компьютере клиента. При этом все мошеннические действия выполнялись невидимо для пользователя.

После отправки мошеннического платежа в банк вредоносная программа предпринимала действия по сокрытию попытки хищения:

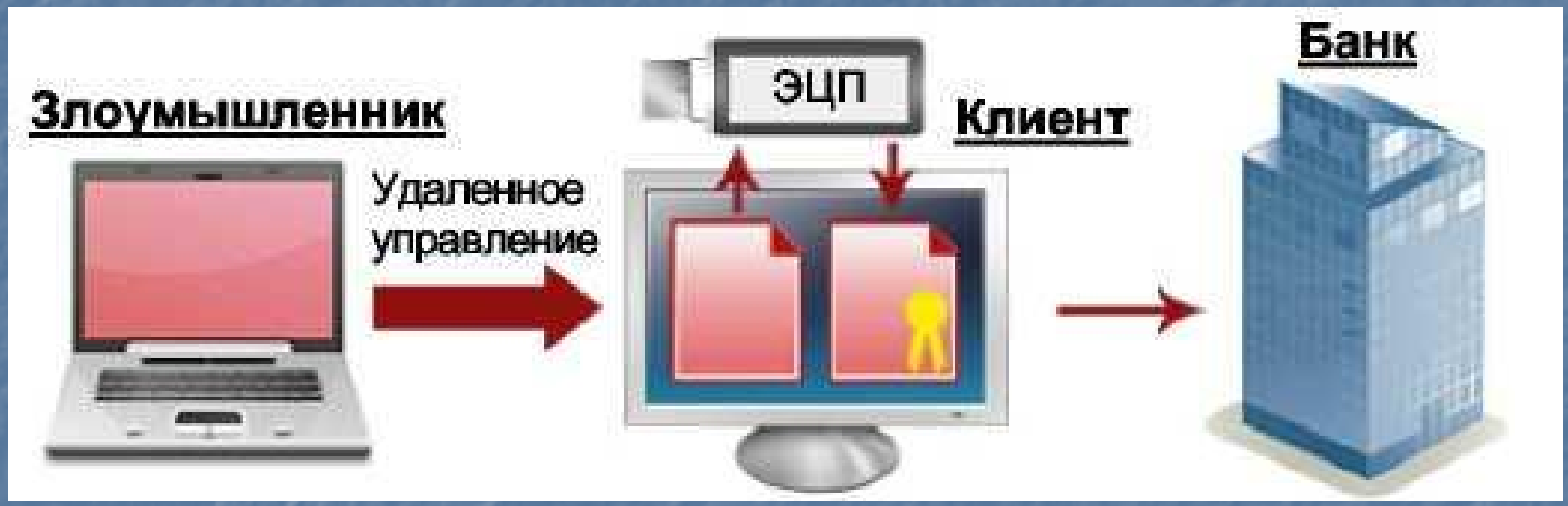
При работе на инфицированном компьютере мошеннический платеж не отображался в списке платежных поручений. При работе с обычного компьютера мошеннический платеж отображался.

При работе на инфицированном компьютере операция списания средств не отображалась в выписке. При работе с обычного компьютера проводка отображалась.

При работе на инфицированном компьютере остаток на счете модифицировался – не уменьшался на сумму мошеннического платежа. При работе с обычного компьютера отображался реальный остаток.

В результате действия вредоносной программы корпоративный клиент не мог с инфицированного компьютера обнаружить факт несанкционированного списания и оперативно помешать злоумышленнику осуществить вывод похищенных средств.

Схема хищения



Кроме того, злоумышленниками в банк по системе ДБО направляются письма от имени клиента с просьбой провести тот или иной документ.

Большая же часть платежей, направляемых злоумышленниками, не вызывает подозрений у банка. Такие документы имеют корректную ЭЦП, обычные реквизиты получателей и типовое назначение платежа для данного клиента. Исполнение банком таких платежей приводит к хищению денежных средств с расчетного счета корпоративного клиента.

Судебная практика показывает, что в случае корректности ЭЦП под правильно оформленным платежным документом Банк не несет ответственности за причиненные убытки.

Для обеспечения аутентичности (целостности и авторства) электронных финансовых документов во всех системах ДБО используется механизм ЭЦП сертифицированный в соответствии с действующим законодательством. Для ЭЦП используется секретный ключ, на основе которого формируется подпись под документом. Подобрать или угадать секретный ключ ЭЦП не представляется возможным.

Секретный ключ ЭЦП находится у только клиента. В банке есть открытый ключ ЭЦП клиента, с помощью которого банковский сервер проверяет подпись клиента под электронными документами. Восстановить из открытого ключа ЭЦП секретный ключ ЭЦП технически невозможно.

Именно поэтому все действия злоумышленников направлены на хищение (использование) секретного ключа ЭЦП у его единственного владельца - клиента.

Анализ выявленных вредоносных программ показывает, что злоумышленники эксплуатируют фундаментальную проблему - неспособность массового пользователя обеспечивать доверенную среду на своем компьютере.

Угрозе хищений секретных ключей ЭЦП клиентов подвержены все системы ДБО, в которых используются секретные ключи вне зависимости от типа носителя - дискета, жесткий диск, флешка, USB-токен или смарт-карта

Причины их возникновения

Сегодня уже нельзя считать компьютер клиента доверенной средой. Особенно компьютер, подключенный к Интернету.

Антивирусы, персональные межсетевые экраны и средства защиты от несанкционированного доступа, безусловно, должны использоваться и своевременно обновляться на компьютере клиента. Но все эти механизмы не гарантируют защиту персонального компьютера клиента от постоянно модифицируемых вредоносных программ.

Причинами возникновения угроз хищений являются:

- Несоблюдение требований информационной безопасности при работе с системами ДБО
- Не соблюдение регламента ограниченного доступа к данному компьютеру
- Использовать и оперативно обновлять системное и прикладное ПО только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений
- Отсутствие или несвоевременное обновление антивирусного программного обеспечения
- Отсутствие средств защиты от несанкционированного доступа из Интернет (межсетевые экраны, политики безопасности)
- Соблюдать правила безопасной работы в Интернете
- USB-токены или смарт-карты подключены к компьютеру не только во время синхронизации и подписи документа при работе с системой «iBank 2»

Средства обеспечения безопасности и меры противодействия новым угрозам в сфере ДБО

Только комплексная защита и соблюдение требований информационной безопасности может снизить риск несанкционированного доступа к системе ДБО

1. Полное и корректное информирование клиентов о новых угрозах
2. Соблюдение правил информационной безопасности, регламента доступа к компьютерам для работы в системе дистанционного банковского обслуживания, и работы с секретными ключами ЭЦП клиента;
3. Перед каждым началом работы в системе «Банк-Клиент» необходимо с помощью антивирусного и другого специального программного обеспечения проверить отсутствие на компьютере вирусов, шпионских и вредоносных программ, отключен ли удаленный доступ к USB-портам и отсутствие удаленного подключения к компьютеру, а также возможности такого подключения. Тем самым обеспечить безопасную среду выполнения программного комплекса «Банк-Клиент».
4. Недопустимость постоянного подключения к компьютеру USB-токенов и смарт-карт «iBank 2 Key». USB-токены и смарт-карты должны быть подключены к компьютеру только во время синхронизации и подписи документа при работе с системой «iBank 2». Не допускается оставлять носитель с ключевой информацией в считывающих устройствах во всех других случаях.

5. При использовании клиентом двух секретных ключей ЭЦП (ключ ЭЦП директора с правом первой подписи, и ключ ЭЦП главного бухгалтера с правом второй подписи) осуществлять работу с системой «iBank 2» на двух отдельных компьютерах с хранением секретных ключей ЭЦП на двух отдельных USB-токенах или смарт-картах.
6. Ключ электронно-цифровой подписи является средством для формирования электронно-цифровой подписи, которая является аналогом собственноручной подписи лица, указанного в карточке с образцами подписей

   Лицо, указанное в карточке с образцами подписей, обязано обеспечить хранение своего ключа электронно-цифровой подписи в недоступном для других лиц месте. Всю полноту ответственности за сохранность ключа электронно-цифровой подписи несет владелец ключа
7. Использование встроенного в систему «iBank 2» механизма дополнительного подтверждения платежных поручений с помощью одноразовых паролей, отправляемых по SMS.

   При включенном механизме дополнительного подтверждения после подписи платежного поручения необходимым количеством ЭЦП документ получает статус «Требует подтверждения». Для перевода документа в статус «Доставлен» клиенту необходимо ввести одноразовый пароль, полученный в SMS-сообщении.

   SMS-сообщение с одноразовым паролем содержит также критичные реквизиты подтверждаемого платежа: сумму, наименование получателя, счет получателя, БИК банка получателя. Это обеспечивает защиту от подмены отображаемых клиенту реквизитов документа вредоносной программой.

   Подтверждение одноразовым паролем в Internet-Банкинге может быть выполнено как сразу после подписания документа, так и позднее. В PC-Банкинге подтверждение документов выполняется в ходе синхронизации.

   К недостаткам SMS относится возможность задержки доставки сообщения по вине сотового оператора. Это может помешать клиенту оперативно войти в систему и совершить важные платежи

8. Дополнительные способы защиты в Internet-Банкинге

- Справочник доверенных получателей;

  Принцип работы механизма доверенных получателей прост: клиент единоразово подтверждает реквизиты (БИК и счет) получателей, которым он доверяет. В дальнейшем при совершении платежей на счет доверенного получателя код подтверждения запрашиваться не будет, даже если сумма платежного поручения превышает установленный банком лимит.

  Клиент может опционально задавать персональные лимиты на каждого доверенного получателя. В этом случае код подтверждения будет запрашиваться при совершении платежа на счет такого получателя, если сумма платежного поручения превышает заданный для него лимит.

  Источниками кодов подтверждения, как и в случае с платежными поручениями, служат SMS-сообщения

- Белые и черные списки получателей

- Дополнительное подтверждение платежей (при превышении лимитов) кодами подтверждений, полученными по SMS

Демонстрация порядка работы системы Банк-Клиент, действий с ключами и дополнительных возможностей по защите от несанкционированного доступа

Порядок действий при подозрении или несанкционированном доступе к системе ДБО

1. В случае возникновения подозрения на неправильную работу программных средств или отказа в работе компьютера (несанкционированная установка пароля на систему Банк-Клиент, нештатная работа или отказ в работе операционной системы или системы ДБО) немедленно обратиться в службу технической поддержки банка для выяснения причин и блокировки системы ДБО.
2. В случае выявления хищения денежных средств в системе ДБО немедленно прекратить любые действия с компьютером, подключенным к системе ДБО, обесточить его (принудительно отключить электропитание в обход штатной процедуры завершения работы, извлечь все аккумуляторные батареи из ноутбука и т.п.) и отключить от информационных сетей (если было подключение, например, по Ethernet, USB, Wi-Fi, Dial-Up и др.). При отсутствии возможности обесточивания ЭУ, осуществить отключение по штатной процедуре и запротоколировать указанный факт.
3. Немедленно обратиться в банк по телефону с заявлением о блокировке системы ДБО, приостановке исполнения платежа и возврате средств. Подготовить письменное заявление об отзыве платежа, возврате средств и блокировании доступа к системе ДБО, а также о компрометации ключей и необходимости смены закрытого ключа. Копия заявления должна быть направлена в банк незамедлительно по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк плательщика течение одного дня.

4. Предпринять меры для обеспечения сохранности и неизменности журналов операционных систем, средств обеспечения и разграничения доступа в сеть Интернет (при наличии таковых) и системы дистанционного банковского обслуживания за максимальный период времени, как до, так и после даты совершения хищения денежных средств.
5. При возможности оперативно обратиться с письменным заявлением к своему Интернет-провайдеру или оператору связи для получения в электронной форме журналов соединений с Интернет с электронного устройства клиента или из его локальной вычислительной сети как минимум за три месяца, предшествовавшие факту хищения денежных средств
6. Зафиксировать действия и события, в том числе имена лиц, имеющих доступ к системе Банк-Клиент, действия с электронными ключами, подключенным к системе ДБО, предшествовавшие факту хищения денежных средств, подготовить объяснения работников клиента об использовании электронных устройств в целях, отличных от осуществления операций в системе ДБО, посещаемых сайтах, о странностях при работе системы Клиент-Банк, перебоях или отказах, обращениях в ИТ-службы, в банк плательщика, о сторонних лицах, побывавших на рабочем месте с системой Клиент-Банк и т.д.
7. В случае выявления хищения денежных средств, обратиться в Банк с заявлением о создании комиссии в соответствии с регламентом соглашения по предоставлению банковских услуг с использованием программно-технического комплекса «БАНК-КЛИЕНТ»

Заключение

Создание максимально защищенной среды для работы с системой Банк-Клиент, использование USB-токенов или Смарт-карт для хранения ключей ЭЦП и формирования подписи под платежным документом, а также использование дополнительных мер по защите от несанкционированного доступа (использование SMS-сообщений с одноразовыми паролями, справочников доверенных получателей и т.д.), дает возможность обеспечить сохранность денежных средств и безопасное использование систем дистанционного банковского обслуживания.

Спасибо за внимание